Identity provider · Keycloak

Set up federation, map the signed identity, and verify a real test sign-in.

https://docs.qintoravacloud.com/integrations/identity-provider/keycloak/

Provider configuration

Issuer template

`{keycloakBaseUrl}/realms/{realm}`

Discovery template

`{keycloakBaseUrl}/realms/{realm}/.well-known/openid-configuration`

Scopes

`openid profile email`

Default claim

`preferred_username`

Default user field

`See provider setup`

Setup

1. Create an OpenID Connect client in the target Keycloak realm.
2. Enable Standard flow and set the exact Valid redirect URI shown below.
3. Use a confidential client and copy its credential secret.
4. Enter the public Keycloak base URL, realm, client ID, and secret.

Field guidance

keycloakBaseUrl

Public HTTPS base URL, for example https://sso.example.com.

realm

Case-sensitive realm name.

clientId

Client ID configured in the realm.

clientSecret

Credential secret for the confidential client.

Verify sign-in

Test metadata and then sign in with an explicitly assigned test user. Confirm the tenant and effective permissions. Test an unassigned account and confirm access is denied. The live demo currently advertises local sign-in.

Federation and SCIM runbook · Provider documentation